Password Managers

Definition

Password managers are programs that securely store website usernames and passwords behind a single master password. Instead of having to remember multiple passwords, you only have to remember one password.

Why Use Them?

- Makes it easier to use strong and unique passwords for every account because you don't have to remember individual passwords. Some password managers generate passwords for you and will alert you if you're reusing passwords across websites.
- Auto-filling of usernames and passwords makes logging in to sites more convenient
- Can help prevent phishing attacks
- Some password managers let you store documents and other information (e.g., addresses, credit card numbers, product keys)

Some Things to Consider When Choosing a Password Manager

- Security model
- Company's track record
- Ease of setup and use
- Price model (free, subscription, one-time fee)
- Compatibility with devices, hardware, software (particularly browsers)
- Account recovery method
- Addons (e.g., tools to identify and fix weak and reused passwords)

Examples of Password Managers

- Bitwarden: https://bitwarden.com/
- Dashlane: https://www.dashlane.com/
- LastPass: https://www.lastpass.com/
- 1Password: https://1password.com/

For a larger list, see https://en.wikipedia.org/wiki/List_of_password_managers.

What about Browser-Based Password Managers?

Most Web browsers offer the option to auto-fill usernames and passwords. Browser-based password managers are limited to the specific browser. So if you use multiple browsers to access your accounts, you'll need to keep multiple password managers up to date. Browser-based password managers are still catching up to third-party password managers when it comes to security and added features.

Risks of Using Password Managers

- Possibility of losing your passwords if you forget your master password (it's important to know your password manager's account recovery methods)
- Attack on password manager can expose all of your passwords

Where to Start?

Try out a couple of password managers with your low-value accounts, i.e. accounts that don't have financial or sensitive information. You might decide that you're comfortable with a password manager storing information about your low-value accounts, but prefer to store information about your high-value accounts elsewhere.

Resources

- Before You Use a Password Manager via Medium: bit.ly/2LJu5Tk
- Password Managers: Under the Hood of Secrets Management via ISE (Independent Security Evaluators): bit.ly/2PzBLZ8
- Choosing Secure Passwords via Schneier on Security: bit.ly/2PAaUMV
- Creating Strong Passwords via EFF (Electronic Frontier Foundation): bit.ly/354Hhts
- Have I Been Pwned? Check if you have an account that has been compromised in a data breach: https://haveibeenpwned.com/